Economics and Management
ISSN: 2367-7600; 1312-594X
Volume: XVII, Issue: 1, Year: 2020, pp. 43-57

APPLICATION OF BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE IN BANK RISK MANAGEMENT

Plamen Dzhaparov[1]

Received: 15.03.2020 Accepted: 30.03.2020

Abstract

The transformation from analogue to digital risk management is becoming a prerequisite in the implementation of the incresingly digital bank institutions' strategies. Among the key steps in this direction is the optimal use of blockchain technology's potential and artificial intelligence. Huge hopes are set on blockchain in view of two key risks facing today's banks: the danger of using the bank system for money laundering and financing terrorism, and cyberattack threat. Artificial intelligence, in turn, creates conditions for processing large arrays of unstructured data risk, more precise identification of potential problems in the future, full automation of manual processes in risk function, credit scoring automation, developing adequate market risk assessment models, etc.

Keywords: *banks, blockchain, artificial intelligence, digitalization, risk management*
JEL Codes: *G210*

1. Introduction

Increasingly, specialized financial literature has been quoting Bill Gates's words: "We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten. Don't let yourself be lulled into inaction." The famous quote is an excellent illustration of the banking industry's current situation. Although they appeared only a decade ago, digital innovations, with blockchain technology, artificial intelligence, business process automation, cloud technologies, augmented reality and other among them, are today a part of the sector's mainstream. Without a shadow of doubt, the simultaneous fundamental transformation of both technology and philosophy of banking leaves a striking impact on each element of credit institutions value change. Viewed from this background, the issue of how these processes reflect upon a risk management that was badly compromised by the financial crisis, evokes a serious research interest.

[1] Chief Assist. Prof., Ph.D., Department of Finance, University of Economics – Varna, pl.djaparov@ue-varna.bg.

It is a fact that for a while digitalization mostly focused on the "customer journey" and its associated processes and operations – marketing, onboarding, service, etc. Later, however, transformations gradually spread to other parts of the organizational structure chain, reaching the risk function as well. But this is not all. With the acceleration of technological innovations and changes, it will most probably be the risk function that will have to develop multiple models and policies to support automated decisions and real-time answers in other parts of the business. Thus, having in mind its inherent simultaneous proximity and connectedness to higher management, the regulatory compliance function and client-orientated organizational units, risk needs to not just adopt and master new technologies, but speed up their implementation, thus turning into "a digital transformation pioneer". Moreover, although the range of digital facilities for risk management in banking is huge, most experts seem to reach a consensus, claiming that the largest and most outstanding potential for risk management transformation is that of blockchain technology and artificial intelligence.

2. Blockchain technology in risk management context

The buzz and euphoria around bitcoin, and other cryptocurrencies that followed, have turned blockchain into one of the most widely commented topics over the last decade. In its most general sense, blockchain technology (BT) is designed to create public records of digital data within the so called distributed ledger (DL) [1]. Each record in the network possesses a unique identification number (hash code) and is also protected by encryption. What is specific in this case is that information is stored on multiple independent computers and servers (called "nodes"), which makes the system fully decentralized. In other words, you do not need a central server to guarantee record authenticity. Instead, control is exercised by individual users, as each of them has a copy of the entire database. Another important peculiarity is s that each change in the system only takes place after a consensus about it (an approval) has been reached by all participants or at least by a certain number of participants."In addition, the distributed ledger also stores transaction chronologies, not just end results (for example, current balances), which protects the system against manipulation and data falsification" (Petrov, 2018, p. 25). Finally, despite its "open" nature, blockchain ensures confidentiality of information. This is so, because encryption by means of complicated techniques guarantees that customers have control over their confidential information and can decide for themselves which third parties should gain access to it by providing a key.

It has rapidly become clear that the possibilities for applying this new technologies far exceed the creation of cryptocurrencies. In view of the revolutionary changes in transaction execution that blockchain "promised", there soon followed accusations that blockchain is nothing but the banking industry's biggest enemy. However, once the initial surge of justified skepticism and anticipated resistance was overcome, at present

banks increasingly "reach for" blockchain in an attempt to take the biggest possible advantage for their business [2].

A survey of 1520 respondents from the financial industry reveals that, according to their expectations, improved risk management (40%) will be the most substantial benefit from BT application, ranking third after better data management (47%) and increased transparency (46%). Following are accelerated digitalization, process rationalization and process automation, cost effectiveness, better security and other (Cognizant, 2019, p. 8). Another survey points out risk reduction, cost cutting and improved effectiveness as the most significant advantages of the financial industry using the so called "smart" contracts (Capgemini, 2016, p. 7) [3].

Where in particular can we look for possibilities to apply blockchain in risk management? Research brings forward the following areas where this new technology can be of use: risk monitoring and risk auditing, taking justified risks, counteragent risk management, fraud risk management (including identity theft prevention), liquidity, capital, system and operational risk management (Infosys, 2019, p. 4). In most of theses areas, however, currently there is a lack of research aiming to measure the real effects of BT implementation. In this sense, expected benefits are rather hypothetical. Nevertheless, in certain spheres affecting risk management, banks are already actively testing blockchain potential.

Thus great hopes are set upon blockchain technology to reduce the risk of using the banking system for money laundering and terrorism financing. In a more narrow aspect, according to research, it has considerable potential for optimizing the execution of "Know your customer" (KYC) procedures [3]. The fact is, banks are currently facing serious difficulties in this area. Their efforts in view of the initial identification of a prospective client's profile frequently result in awkward, cumbersome and ineffective onboarding processes [4]. In addition, many customers are disappointed with the large volume of confidential information their bank partners require. Banks are also increasingly worried by the growing Compliance costs that accompany KYC regulations. Last, but not least, as the requirements for investigating customers are much too complex and subject to various interpretations, compliance often becomes an overwhelming task (Carmichael, 2018, p. 1).

The abilities of blockchain technology to overcome these challenges are assessed in view of the key characteristics of the said technology. Thus, for example, when a customer presents information to a particular bank that belongs to a blockchain-based KYC platform, data are also replicated to all the other creditors participating in the platform [5]. On this basis, the key benefit for banks is cost cutting and shortening the time for collecting, validating, storing and moving information. Therefore, institutions with long-standing connections with a given customer, will considerably facilitate this customer's initial identification in another institution, eliminating time-consuming and annoying manual checks (for instance verifying the authenticity of the copies of personal

documents presented) (Thomson Reuters, 2018, p. 6). This will also greatly contribute to increasing customer satisfaction, as it will no longer be necessary to provide the same information again and again. Apart from everything else, simplification of onboarding processes could lead to a quicker access to new customers and better customer relations management, which in turn could save banks more time and resources (Carmichael, 2018, p. 5).

As for the follow-up monitoring, the unique identifier allows credit institutions within the network to automatically receive updates on customer information and their risk exposure (Thomson Reuters, 2018, p. 7). This automation, combined with higher transparency and more comprehensive customer information, will reduce credit risk (counteragent risk). In addition, the number of transactions wrongly considered suspicious will reduce, and, respectively, the need for manual interference will be limited. According to even braver forecasts, in this aspect blockchain technology can help for reducing the number of employees by 30%, which in turn could ensure around $1.4 bn cost economies for banks (Goldman Sachs, 2016, p. 75).

Distributed digital ledgers will also contribute to compliance-risk minimization, as all transactions referring to a particular customer can be automatically followed and, consequently, this information can be used as evidence that the bank has acted in compliance with the requirements of the AML- legislation. Thus, over time, the fact that customer information is becoming easier to verify, could potentially reduce the fines imposed upon financial institutions (Goldman Sachs, 2016, p. 74).

Against this background we can conclude that from the KYC process view point, blockchain technology is able to stand as a solid foundation for a secure, effective and decentralized platform for collecting, validating and sharing the necessary customer information. Summarized, its advantages appear to be as follows: possibility for sharing insider negative customer information, generated by individual financial institutions; verification of information arrays (array integrity checking, deleting superfluous records, adding data); forming a more-realistic idea of the customer risk profile (by discovering relationships with other risky persons, which had remained undetected by conventional software); better monitoring opportunity (as a change in customer risk profile is recorded by even a single financial institution in the network, owing to blockchain, this change becomes automatically visible to all participants)“ (Valkanov, 2019a, p. 211-212).

From the point of risk management, another important advantage of a blockchain network is its “genetically inherent” resilience to cyberattacks. Though not “immune” against all forms of cyber risk, blockchain’s unique structure provides certain protection mechanisms which are not inherent to conventional IT systems and technologies (English, Kim & Nonaka, 2018, p. 11-12):

To begin with, blockchain’s decentralized and distributed structure is an advantage that can deter cybercrime or at least minimize its negative impact. This is so, because hackers typically target their attacks at a centralized data base, which, once hacked,

infects and destabilizes the whole system. In contrast, here an attack against one or a few participants in the system cannot in any way pose a risk to the ledger stored in the nodes, which were not attacked. In this sense, the distributed network structure could ensure a higher operational resistance for the bank. Moreover, even if there were a real attack, the system's distributed character can facilitate data- and- process restoration (assuming that not all nodes are simultaneously damaged). In turn, this possibility will reduce the need for costly restoration plans (European Investment Bank, 2019, p. 28).

Secondly, the consensus mechanism that is fundamental to blockchain requires that a certain number of participants reach consensus about whether the newly created data block is valid and fit to be included in the joint ledger, as well as whether the ledger itself, with all its history corresponds to the network validation rules. In this sense hackers will have to "beat" the consensus mechanism, by manipulating a sufficient number of nodes in the network and thus forge the ledger. However, blockchain can easily compromise the success of such an attack, if the network contains a sufficient number of nodes and transaction validation calls for a considerable degree of consensus among them.

Thirdly, blockchain technology makes use of various forms of encryption in various points, thus providing a multi-layer protection against cybersecurity threats.

In the fourth place, blockchain network transparency also provides protection against virtual attacks, creating a serious difficulty for hackers to implement unnoticed malware to collect information and transfer it to another database (managed by them). The reason is that every participant has at their disposal an identical copy of the ledger, which is a prerequisite for considerably easier record tracking. In this sense any deviations from the system's normal rhythm (for example, those caused by malware installed) can be quickly identified. In addition, information gained from such an event can be "implanted" in conventional security devices, such as Firewalls and Intrusion detection system, with which cybersecurity could be improved in the future (Deloitte, 2016a, p. 14).

Fifth, blockchains are often hosted on cloud platforms that have solid cybersecurity controls. Cloud computations offer participants an easily accessible and sustainable platform, which results into a shorter stay in the system, less transaction loss risk, and lower likelihood of not reaching consensus.

3. The possibilities of artificial intelligence

Artificial intelligence in its various forms and performance has been gaining popularity with banks [6]. Defined as "a comprehensive term referring to the capabilities of a machine to perform cognitive functions associated with the human mind, including perception, reasoning, learning, interaction with the environment, problem-solving and

even creativity", there are dozens of smart technologies and activities that are associated with AI. The more important of these are:

- predictive analytics;
- machine learning, ML;
- robotic process automation, RPA;
- artificial neural networks;
- natural language processing, NLP;
- computer vision and other.

A survey among over 2000 respondents from the financial industry at the end of 2018 finds out these AI technologies are mostly applied in the following spheres: automation of manual processes, credit scoring, data cleaning and improvement, risk ranking, model validation and model calibration. According to authors, survey results definitely confirm financial institutions' ever stronger interest in artificial intelligence and mainly in its abilities to optimize risk functions (GARP, 2019, p. 3-7). This is hardly surprising given the forecasts that this new technology's application in risk management will save banks $ 31bn by 2030 (Ginimachine, 2018).

More particularly, the benefits of applying artificial intelligence for the purposes of bank risk management are incomparable. The enormous computing power it offers allows for the processing of large arrays of information in a short time, and more importantly, the abilities of advanced analytics algorithms to retrieve much more meaningful and usefulin formation out of the "ocean" of *unstructured data* [7]. In parallel, its capacity for decision-making, based on complicated statistical methods, instead of clearly pre-defined rules, creates prerequisites for avoiding incorrect risk forecasts, often followed by billions in losses for credit institutions.Against this background, robotic process automation, machine learning and natural language processing have the potential to improve effectiveness in a number of processes, among them approval and loan granting, risk aggregation, assessment of varios risk factors impact upon the formation and allocation of profits, losses, etc. In addition, these new algorithms ensure end-to-end transparency, i.e. at any given moment it will be clear whois responsible at the concrete stage of the processes of identification, assessment and various type of risk management.

Smart platforms and applications can perform precise and timely assessment of risks emerged in previous periods and on that basis identify early symptoms of potential future problems and threats, Therefore, owing to the more realistic scenarios drawn up, other key issues in risk management will be improved, such as stress- tests and "What if" type of analyses (Genpact, 2018, p. 8). No less important is the role of artificial intelligence in fraudulent practices identification and prevention. The fact is banks already use specially programmed systems (for instance, to identify credit card fraud), whose basic task is to block doubtful transactions. The future, however, promises a considerable expansion of this potential, as with time, in the process of self-learning, technologies will get smarter and smarter and will be able to detect and prevent

increasingly more sophisticated fraudulent schemes - an advantage, which according to research, is likely to have the biggest impact on risk management in the foreseeable future [8].

Compliance risk management will also be simplified due to the intelligent workstations, which consolidate contact points, direct queries to the experts in charge and increase transparency and access (BCG, 2019). Something more, especially in the field of compliance, new technologies give financial institution unload to some degree by the burdensome regulatory costs imposed by fast changing regulatory framework (Valkanov, 2019b, p. 28). Another circumstance not to be ignored is that artificial intelligence – based technologies overcome various kinds of bias and subjectivity pertaining to humans. This advantage is particularly valuable from the standpoint of the lessons learned during the global financial crisis, which revealed that more often than not, bank problems result from intentional disregard for risk rules and limits on the part of executives and employees in charge [9]. Artificial intelligence benefits can also be sought in terms of image. The ever more active implementation of such technologies and platforms in risk management could be interpreted by the public as a sign of the particular bank's reliability and security as an institution that effectively and appropriately manages its risks. Besides, customers will be aware that the bank is willing to transform and has the necessary capacity to fight the competition of emerging hich-tech financial companies (neobanks, FinTech companies, etc). This is a particularly crucial point for the new high-tech generations.

Next, artificial intelligence offers a large number of new possibilities for the *automation* many manual and standardized processes in all categories of risk management, and in particular for the so called Robotic process automation (RPA). Tracking risk limit breach, risk data quality assessment and reporting documents preparation are but a few of the examples in this area. Among the most significant benefits of risk management automation there stand out saving time, reduced need for manual interference, fewer mistakes, compliance costs reduction, risk reports generation in (almost) real time, better control over processes, maintaining the operational flexibility necessary and improving system effectiveness. In addition, the development of automated models allows risk teams to test a large amount of output data by parallel simulations, choose the most accurate ones and use the time saved to solve other important business problems (BCG, 2019) [10].

RPA technology is considered particularly useful for minimizing exponentially growing compliance risk. Thus, for example, a global British bank reports that in the recent past it took considerable resources to manually track regulatory changes in over 300 websites a day and their subsequent input in risk and compliance models. A typical employee used 15% of their time on similar activities. At the present stage, the larger part of these manual activities are automated with the help of software robots, The bank can now quickly and effectively "catch" various regulatory information from multiple public

websites – from stock exchanges (NYSE, Euronext) to the Federal regulatory agencies (Kofax, 2018, p. 10). Robots work alongside bank employees to perform their basic task – follow various sites – from stock exchanges to federal regulatory agencies. From the point of view of compliance risk there are other benefits of RPA that should not be underrated: coordination between risk management teams and those engaged in compliance with regulations, avoiding fines and reputational damages; providing comprehensive and accurate information for auditors.

The application of artificial intelligence in risk management also has the potential to contribute to building interactive and personalized platforms and augmented reality interfaces for the customer. Intelligent vision technologies allow users a more intutitive access to smart business applications and solutions, with which to better understand their costs and financing capacity.In mobile applications and bank websites, for instance, users could view their cost history and other information intuitively, without having to accumulate it by analysis of various invoices and receipts and without having to formulate a vision of their own cost models by themselves.

It is also crystal clear that transparency and argumentation of the decision made about the customer risk profile (for instance, why they have been refused a loan) are key factors for customer satisfaction. With the help of artificial intelligence banks could equip their interfaces with functionalities allowing customers to change the parameters of the serveices they use (for instance, set different loan amounts) and trace in real time the direct consequences of these changes. One of the most advanced vision technologies, which can enhance customer experience, is Augmented Reality, where information is "digitally overlaid" on real environment. This can mean, for instance, that customers receive risk-related information as overlays upon objects they wish to purchase. Thus, in case of mortgages, or automobile loans, customers will receive information about their available funds, about how the amount suggested can be used for other portfolio positions, about the most appropriate maturity date, about amounts of potential credit and other (IIF, McKinsey, 2017, p. 50-52).

Let us now discuss the application of AI algorithms in the management of certain risk categories that are of key importance for banks. All analysts agree that credit risk managemnt is the area that will most benefit from artificial ntelligence. Apart from providing a faster assessment of the potential borrower at a lower cost, the credit scoring performed by intelligent machines is based on more sophisticated rules and algorithms compared to to those employed in the conventional credit scoring models. Although at present a potential borrower check can also be performed in more or less real time, the data it is based on are periodically (usually monthly) updated. But in the era of open banking and Big Data this definitely doesn't seem enough. It is exactly here that a machine learning platform can momentarily draw information from various sources at the same time – for example, other suppliers of financial and non- financial services, public registers, social networks, etc. and make a decision based on real- time customer data

[11]. On this ground the system can determine the suitable product for the customer according to the prosspoint between customer's risk profile and the bank's risk appetite.

In the end, the more accurate, faster and cheaper customer segmentation according to their credit quality will result in a shorter credit decision making process. Applying machine learning algorithms in credit scoring may also bring about greater access to credit. Under conventional assessment model, in use on most markets, a potential borrower must possess enough information on their credit history that can be assessed. Should such information be missing, no credit rating can be generated and prospective credit-worthy borrowers are often not granted a loan and thus a chance to form their own credit history. By using altenative data sources and applying machine learning algorithms this problem should be solved (FSB, 2017, p. 12). In turn, natural language processing technology could recognize any suspicious data received when the application form was submitted, and biometric technologies could identify malware. Thus artificial intelligence suggests a potential to save millions in "fraudulent or bad" credit applications and at the same time ensures that good credit quality customers will get the best product possible under their own circumstances and in a perfectly clear application process (Accenture, 2018, p. 17). According to McKinsey's study, in addition, better credit models can improve bank return in four ways: higher interest revenue from the credit business; improved risk monitoring; lower operating and sales costs; higher effectiveness and higher return on capital (McKinsey, 2017).

Some analysts believe that AI also offers numerous possibilities for operational risk management. One of these is risk event classification. A computer algorithm, for example, can read risk specifications, written by risk managers, and group and rank them according to their impact and frequency. Combining historical loss data with risk reports can lead to a more accurate future loss forecasting (Consultancy.ey, 2019). Financial institutions can also use automated smart systems to observe their employees (traders), by linking purely trade information with other behavioural data, such as e-mail messages, events in the calendar, the time one arrives and leaves the office building and even telephone calls. Artificial intelligence-based analytics platforms can also manage suppliers risk by integrating various information about them – from their geographical and geopolitical environment to their financial risk, sustainability and corporate social responsibility, Artificial intelligence systems can also be taught to detect, track and repel cyberattacks. In particular, they will be able to identify software with certain distinctive features (for instance, with an ability to consume a large amount of processing power or forward too many data) and then block the attack (Boillet, 2018).

As for market risk, machine learning has considerable potential in all stages of the development of an adequate market risk assessment model.Thus, during the preparation of the set of data that is necessary for modelling, ML-techniques can be used for retrieving and cleansing of relevant macroeconomic variables or historical data on key trading tools. When choosing a particular model methodology the focus is on using

machine learning algorithms for improving forecast accuracy or on developing trade strategies for tfinancial markets. ML-techniques can also be applied in the stage of final model testing and model validation, for example, for defining the suitable threshholds and benchmark indicators necessary for monitoring model effectiveness (Kumar, 2018, p. 3-4) [12].

In view of what has been discussed so far, according to some predictions, the increasingly wider proliferation of artificial intelligence within the risk function will probably go through three stages. Initially it will be used for accumulating valuable data that are necessary for the deeper understanding of risks and threats, which in turn will enable a more informed decision-making. The second stage will include AI application in monitoring and risk supervision aimed at providing standards and controls, under which risk activities may be performed. In parallel, this will provide an opportunity to study certain specific cases of risk taking, so as to guarantee these cases match the established frameworks and standards. Having reached maturity, artificial intelligence is highly likely to to be actively used for the provision of an independent standpoint concerning key risk decisions and an independent challenging the decisions made by the first line of protection (business units). In short, at present AI can provide information to assist risk managers; with time it will gradually develop, evolving to a programming algorithm for low class decision-makung, and at a later stage to advanced applications for performing independent checks on processes (Jogi, 2018).

4. Conclusion

Blockchain and artificial intelligence are two of the technologies that have the potential to fundamentally transform banking risk management. Their application can provide benefits to credit institutions in a number of areas: Big Data processing, customer segmentation, credit scoring, fraud prevention, regulatory compliance, risk modeling, cybersecurity, AML processes, market risk forecasting, etc. However, in order to make the most of this potential, banks must not only "equip" themselves with good IT professionals, infrastructures and systems, but also implement these new technologies at the heart of their risk strategies and policies. It also requires a radical change in the thinking and behavior of banking risk management.

ENDNOTES

[1] The terms “blockchain“ and “distributed ledger technology“ (DLT) are frequently used as interchangeable, but the fact is there is considerable difference between them. DLT is a “family” of technologies which use distributed database architecture with the aim of supporting multiple identical copies of a verifiable, distributed or decentralized transaction and data register. Blockchain is a specific type of DLT and

a method of organizing data into aggregated ordered blocks which are "tied together" by means of cryptographic hash function (English et al., 2018, p. 6).

[2] Thus at the end of 2018 it became clear that more than 75 of the world's largest banks will participate in the initiative Interbank Information Network (IIN) – the largest blockchain payment application to be used by the regulated banking industry so far. The aim of this common and distributed ledger, which all the banks will have access to, is for banks to be able in real time to solve problems such as Compliance-checks, missing information, wrong addresses,etc., which at present frequently result in delaying transactions for days and weeks (Noonan, 2018). In the middle of 2019 information appeared stating that 14 of the global banking institutions, UBS, Credit Suisse, Barclays, MUFG Bank among them, have invested $ 63 m in the creation of a BT- based crypto-token - Utility Settlement Coin (USC), which should facilitate and accelerate cross-border payments. In this sense USC does not aim to be the next decentralized cryptocurrency, but would rather function as an instrument for improving bank effectiveness (Pollock, 2019).

[3] With the coming into force of the Directive on the prevention of the use of the financial system for money laundering and terrorist financing in 2017, banks are already obliged to have a developed Know Your Customer (KYC) policy. According to regulatory requirements, they have to prepare a detailed risk profile of each potential customer and determine the risk category these customers fall in. It is also necessary for banks, during the process of servicing the customer, to gather current client information concerning client habitual activity, so as to be able to identify suspicious operations, which go beyond the framework of the customer profile built. In particular, the basic elements the KYC process should contain are as follows: customer approval policy, customer identification procedures, transaction monitoring, risk management.

[4] According to computations, due diligence-practices, applied in order to comply with the regulatory requirements concerning KYC procedures, are presently taking 24 days on average. In certain cases this serious delay can lead to a $25000 potential revenue loss from a single customer, as a result of the impossibility to carry out a cross sale, for example (Cognizant, 2019, p. 9).

[5] But although information storage is essentially decentralized, another bank will not have access to it (in fact, it will not even know such information exists), unless it is explicitly authorized by the customer in the form of a decryption key. Besides, reliable tracing the separate "blocks in the chain" allows customers to find out which banks have gained access to their information. Therefore, blockchain practically creates a personal data confidentiality model, whereby the customer retains full control over them.

[6] According to a forecast by the American market research consultants International Data Corporation, in 2019 banks will invest $ 5,6 bn in the introduction of AI-based

decisions. Globally in this field they will come second only to retailers with investments of $ 5,9 bn, but Western Europe will retain the leading position in the field (IDC, 2019).

[7] In other words, artificial intelligence and risk management are in perfect partnership when there is a need for unstructured data processing and evaluation. For this reason, in view of expert prognoses that "by 2025 over 80% of the world's data will be unstructured" (Capgemini, 2018), the incredible potential of AI shows through, even if we only consider the above example.

[8] At present the most widely applied method for identifying fraud is using computers to compare a particular set of structured data against a set of banking rules and limitations, for example, a maximum threshold of $10000 is set for electronic transfers and every transaction worth above the said sum is marked by the computer as suspicious and is liable to further investigation. The problem here is that this type of structured data analysis often generates too many false positive results, which entails many hours of painstaking investigation. Now, with the help of cognitive analyses fraud identifying models can become much more secure and accurate. "If a cognitive system identifies a certain transaction as potential fraud, but a human later finds out this is not the case, the computer learns from human insight and will not make the same mistake again, In other words, the computer becomes ever more intelligent. This is an enormous change in the "rules of the game", as in this way new technologies can help identify emerging behavioural models and original fraudulent schemes, which could never be detected by humans" (Deloitte, 2016b, p. 2-3).

[9] Of course, we should not underestimate other opinions, claiming that machines assess reality the same way humans do: by seeing many cases from the reality and adjusting their behavior according to predictions and past experience. In this aspect, they, too, can be viewed as biased and unobjective.

[10] Banks that are more advanced in implementing automation declare that their projects performed 70 to 80% more effectively in manual, repetitive tasks (such as an automated system for tracking collaterals, detecting and cleansing data anomalies, etc) (IIF, Ernst & Young, 2018, p. 23).

[11] In addition to everything else, the computer processing of this new data constellation provides an opportunity to augment customer risk profile with certain qualitative factors such as consumer behavior and willingness to pay (FSB, 2017, p. 12).

[12] An interesting example of using machine learning in developing a model for market risk assessment can be seen in the activities of the French investment intermediary Nataxis, which, in verifying their model uses unsupervised learning algorithms. While this algorithm was being tested, every night these algorithms performed over 3 million calculations, aiming to establish new types of links between the assets traded on the market and the identification of the anomalies in the forecasts the company produced. Thus, identifying wrong results in the stress tests used, ML-algorithms turn

into a valuable instrument for monitoring, validation and correction of the investmen intermediary's current stress tests and trading models (Woodall, 2017).

REFERENCES

Accenture (2018). *Redefine Banking with Arteficial Intelligence*, https://www.accenture.com/_acnmedia/pdf-68/accenture-redefine-banking.pdf.

BCG (2019). *Global Risk 2019: Creating a More Digital, Resilient Bank*, https://www.bcg.com/publications/2019/global-risk-creating-digital-resilient-bank.aspx.

Boillet (2018). *Why AI is both a risk and a way to manage risk*, https://www.ey.com/en_gl/assurance/why-ai-is-both-a-risk-and-a-way-to-manage-risk.

Capgemini (2016). *Smart Contracts in Financial Services: Getting from Hype to Reality*, https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0.pdf.

Capgemini (2018). *Organizations need to give unstructured data its rightful place if they want to get value out of data*, https://www.capgemini.com/2018/08/reorganizing-unstructured-data/.

Carmichael, A. (2018). *INSIGHT: Blockchain Helps Banks Streamline Know Your Customer Processes*, https://application-production.cdn.ranenetwork.com/blog/wp-content/uploads/2018/08/02160355/Blockchain-Helps-Banks-Streamline-Know-Your-Customer-Processes.pdf.

Cognizant (2017). *Financial Services: Building Blockchain One Block at a Time*, https://www.cognizant.com/whitepapers/financial-services-building-blockchain-one-block-at-a-time-codex2742.pdf.

Consultancy.eu (2019). *AI can improve operational risk management in banking*, https://www.consultancy.eu/news/2571/ai-can-improve-operational-risk-management-in-banking.

Deloitte (2016a). *Taking cyber risk management to the next level*, https://www2.deloitte.com/tr/en/pages/risk/articles/cyber-risk-management-financial-services-industry.html.

Deloitte (2016b). *Why artificial intelligence is a game changer for risk management*, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-ai-risk-powers-performance.pdf.

English, E., Kim, A.D. & Nonaka, M. (2018). *Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry*.

European Investment Bank (2019). *Blockchain, FinTechs and their relevance for international financial institutions*, https://www.eib.org/attachments/efs/economics_working_paper_2019_01_en.pdf.

FSB (2017). *Artificial intelligence and machine learning in financial services: Market developments and financial stability implications*, https://www.fsb.org/wp-content/uploads/P011117.pdf.

GARP (2019). *Artificial intelligence in banking and risk management: Keeping Pace and Reaping Benefits in a New Age of Analytics*, https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/third-party-whitepapers/en/artificial-intelligence-banking-risk-management-110277.pdf.

Genpact (2018). *Transforming strategic risk management to realize competitive advantage: Genpact/ERMC FS Risk Management Survey*, https://www.genpact.com/ downloadable-content/insight/transforming-strategic-risk-management-to-realize-competitive -advantage.pdf.

Ginimachine (2018). *Banking Today: Risk Management with AI*, https://ginimachine.com/blog/banking-today-risk-management-with-ai/.

Goldman Sachs (2016). *Profiles in Innovation: Blockchain*, https://www.finyear.com/attachment/690548/.

IDC (2019). *Worldwide Spending on Artificial Intelligence Systems Will Grow to Nearly $35.8 Billion in 2019*, https://www.idc.com/getdoc.jsp?containerId=prUS44911419.

IIF, Ernst&Young (2018). *Accelerating digital transformation: Four imperatives for risk management*, https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-ninth-annual-iif-bank-risk-survey-accelerating-digital-transformation.pdf.

IIF, McKinsey (2017). *The future of risk management in the digital era*, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20future%20of%20risk%20management%20in%20the%20digital%20era/Future-of-risk-management-in-the-digital-era-IIF-and-McKinsey.ashx.

Infosys (2019). *Blockchain adoption in financial services*, https://www.infosys.com/industries/financial-services/white-papers/Documents/blockchain-adoption-financial-services.pdf.

Jogi (2018). *Artificial Intelligence Reshaping Risk Management In The BFSI Sector*, https://www.expresscomputer.in/artificial-intelligence-ai/artificial-intelligence-reshaping-risk-management-in-the-bfsi-sector/30773/.

Kofax (2018). *Forecasting your future: How Financial Institutions Are Improving Operations*, https://badr.blog/wp-content/uploads/2018/09/kofax-kapow-how-financial-institutions-are-improving-operations-with-rpa-ebook.pdf.

Kumar (2018). *Machine Learning for Model Development in Market Risk*.

McKinsey Analytics. An executive's guide to AI, https://www.mckinsey.com/ business-functions/mckinsey-analytics/our-insights/an-executives-guide-to-ai.

Morrison, A. (2016). *How smart contracts automate digital business*, https://usblogs.pwc.com/emerging-technology/how-smart-contracts-automate-digital-business/.

Noonan, L. (2018). *JPMorgan widens blockchain payments to more than 75 banks*, https://www.ft.com/content/41bb140e-bc53-11e8-94b2-17176fbf93f5.

Petrov, D. (2018). *Application of Blockchain and Smart Contracts in the Financial Industry (In Bulgarian)*. Izvestia - Journal of the Union of scientists – Varna, Economic sciences series, vol.7, №2, pp. 24 - 33.

Pollock, D. (2019). *World's Biggest Banks Splash $63 million on a Blockchain Digital Currency*, https://www.ccn.com/biggest-banks-63-million-blockchain-digital-currency/.

Thomson Reuters (2018). *A Blockchain Enabled KYC Solution: New Horizon or False Dawn?*, https://www.refinitiv.com/content/dam/marketing/en_us/documents/white-papers/kyc-blockchain-white-paper.pdf.

Valkanov, N. (2019a). *Compliance v pomosht na finansovoto regulirane (in Bulgarian)*. Varna: Science and Economy, Library "Prof. Ts. Kalyandziev", Book 59, 335 p., ISBN 978-954- 21-0994-5.

Valkanov, N. (2019b). *Mitigation of regulations burden in financial sector by application of high tech solutions*. Journal for Economics and Management science of Faculty of Economics – South-Western University – Blagoevgrad, Volume: XVI, Issue: 1, Year: 2019, pp. 19-30. ISSN: 2367-7600; 1312-594X, http://em.swu.bg/images/SpisanieIkonomikaupload/Spisanieikonomika2019/MITIGATION%20OF%20REGULATIONS%20BURDEN%20IN%20FINANCIAL%20SECTOR.pdf.

Woodall, L. (2017). *Model risk managers eye benefits of machine learning*, https://www.risk.net/risk-management/4646956/model-risk-managers-eye-benefits-of-machine-learning.